IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

JUERGEN NOWOTTNICK ET AL

Atty. Docket

DE 010002

Serial No.

Group Art Unit

Filed: CONCURRENTLY

Ex.

Title: ACCESS SYSTEM WITH POSSIBILITY OF LEARNING UNKNOWN ACCESS KEYS

Commissioner for Patents
Washington, D.C. 20231

AUTHORIZATION PURSUANT TO 37 CFR §1.136(a)(3)
AND TO CHARGE DEPOSIT ACCOUNT

Sir:

The Commissioner is hereby requested and authorized to treat any concurrent or future reply in this application requiring a petition for extension of time for its timely submission, as incorporating a petition for extension of time for the appropriate length of time.

Please charge any additional fees which may now or in the future be required in this application, including extension of time fees, but excluding the issue fee unless explicitly requested to do so, and credit any overpayment, to Deposit Account No. 14-1270.

Respectfully submitted,

By _____
Edward W. Goodman, Reg. 28,613
Attorney
(914) 333-9611

DE 01000024

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	100 41 557.1
Anmeldetag:	24. August 2000
Anmelder/Inhaber:	Philips Corporate Intellectual Property GmbH, Hamburg/DE
Bezeichnung:	Zugangssystem mit Anlernmöglichkeit fremder Zugangsschlüssel
IPC:	E 05 B 47/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 12. April 2001
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Agurks

CERTIFIED COPY OF PRIORITY DOCUMENT

A 9161

BESCHREIBUNG

Zugangssystem mit Anlernmöglichkeit fremder Zugangsschlüssel

1. Anwendungsgebiete der Erfindung

Für Zugangssysteme basierend auf einem Authentisierungsverfahren wird eine Möglichkeit gegeben, einen Bereich für weitere Personen frei zu geben und diese gewährte Zugangsmöglichkeit auch wieder zu entziehen.

Diese Personalisierung kann ohne Hilfe eines Systembetreibers, des Herstellers oder anderer autorisierter Stellen erfolgen. Es handelt sich dabei um Zugangssysteme ohne hierarchische Struktur, wie sie etwa für Fahrzeuge oder Wohnungen angewendet werden. Diese Systeme verfügen i.A. nicht über die Möglichkeit eines kryptographisch sicheren Schlüsselaustauschverfahrens, das eine einfache Erweiterung des Zugangsbereiches einzelner Schlüssel ermöglichen würde.

Mit Hilfe des vorgestellten Verfahrens kann eine flexible Verwaltung der autorisierten Personen für einen bestimmten Zugangsbereich realisiert werden, die von den bereits autorisierten Personen in einfacher Art und Weise durchgeführt werden kann.

2. Stand der Technik

Die Realisierung von nicht-hierarchischen Schließsystemen sieht gegenwärtig keine Möglichkeit der dedizierten Erweiterung des autorisierten Bereiches eines Schlüssels vor. Bei oben beschriebenen Zugangssystemen wird üblicherweise eine Anzahl von autorisierten Schlüsseln für ein Schloss vom Hersteller oder einer anderen berechtigten Stelle produziert. Es gibt keine Möglichkeit weitere Schlüssel, welche bereits für einen anderes Schloss autorisiert sind, für ein weiteres Schloss zu autorisieren, ohne auf die Mithilfe von Servicepersonal angewiesen zu sein.

Dabei wird im allgemeinen ab Werk jeder Schlüssel nur für ein bestimmtes Schloss konfiguriert und hat keine Möglichkeit, sich bei weiteren Schlössern autorisieren zu lassen.

Probleme bei den im Markt befindlichen Systemen sind die fehlende Flexibilität und der damit verbundene hohe Verwaltungsaufwand sowie die relativ hohen Kosten für die anfallenden Serviceleistungen vor Ort.

3. Beschreibung der Erfindung

Das vorgeschlagene Verfahren soll anhand eines Beispiels aus der Automobilindustrie beschrieben werden, läßt sich aber ohne weiteres auf alle Zugangssysteme übertragen, welche die unten beschriebenen Voraussetzungen erfüllen.

3.1 Definitionen

Im folgenden sollen folgende Abkürzungen verwendet werden:

F..... Fahrzeug

S..... Fahrzeugschlüssel

BS..... Besitzer-Schlüssel (Fahrzeugschlüssel mit speziellen Fähigkeiten)

K.....kryptographisch benutzter Schlüssel, welcher im Fahrzeug und im Schlüssel gespeichert ist (geheimer Schlüssel)

Id..... Bezeichner (Identifier)

Außerdem steht „x" für eine beliebige natürliche Zahl und „*" für einen beliebigen Buchstaben.

Dabei beschreiben gleiche Nummern die ab Werk konfigurierte Zusammengehörigkeit. Z.B. gehört K1 zum Kryptosystem von F1 und S1. Die verschiedenen zu einem Fahrzeug F1 gehörigen Schlüssel seien mit S1a, S1b usw. oder allgemein mit S1* bezeichnet.

3.2 Voraussetzungen

V1. Jeder Schlüssel Sx ist mit einem eindeutigen Bezeichner Id(Sx) ausgestattet, der den Schlüssel von allen anderen Schlüsseln des gesamten Systems unterscheidet.

V2. Zu jedem Fahrzeug gehören ab Werk eine Anzahl von Schlüsseln, mit welchen sich nur dieses Fahrzeug bedienen läßt (üblicherweise Öffnen und Starten). In jedem dieser Schlüssel ist somit der gleiche geheime Schlüssel gespeichert, wie im zugehörigen Fahrzeug.

V3. Das Fahrzeug F1 hat alle Bezeichner der für Fahrzeug F1 autorisierten Schlüssel Id(S1*) gespeichert und läßt nur gespeicherte Bezeichner für eine Authentisierung zu.

V4. Um das Fahrzeug F1 bedienen zu können, muß zwischen Fahrzeug F1 und dem Schlüssel S1 eine erfolgreiche gegenseitige Authentisierung erfolgen. Diese basiert auf einem symmetrischen kryptographischen Algorithmus, dessen kryptographische Stärke auf dem nur Fahrzeug F1 und Schlüssel S1 bekannten kryptographischen Schlüssel K1 beruht. (Eventuell hat der Hersteller die geheimen Schlüssel gespeichert, diese sind aber als sicher verwahrt vorausgesetzt.) Als Algorithmus wird ein sog. „Challenge-Response-Verfahren" vorausgesetzt, welches zu einer gegenseitigen Authentisierung erweitert wurde. Damit wird gleichzeitig vorausgesetzt, daß eine der beiden Seiten (Fahrzeug F1 oder Schlüssel S1) Zufallszahlen („Challenge") von hinreichender Qualität erzeugen kann. Für den hier beschriebenen Fall wird davon ausgegangen, daß Fahrzeug F1 in der Lage ist entsprechende Zufallszahlen zu erzeugen.

V5. Sowohl Fahrzeug als auch Schlüssel verfügen intern über denselben Pseudo-Zufallszahlengenerator (welcher sich ggf. aus dem schon benutzten symmetrischen kryptographischen Algorithmus ableiten läßt).

V6. Es existiert kein geheimer Schlüssel K, welchen sich ab Werk verschiedene Schlüssel S teilen. Insbesondere gibt es keinen sogenannten „Generalschlüssel", der allen Schlüsseln Sx bzw. Fahrzeugen Fx bekannt ist.

3.3 *Zusatzvoraussetzung*

V7. Die einem Fahrzeug F1 ab Werk zugeordneten Schlüssel S1a, S1b, ... unterscheiden sich hinsichtlich der Berechtigung weitere Schlüssel anzulernen. Im weiteren soll es nur den als Besitzerschlüssel (BS1*) bezeichneten Schlüsseln möglich sein, das beschriebene Verfahren zu initiieren.

V7 stellt prinzipiell keine Bedingung an das beschriebene Verfahren, erleichtert aber die Realisierung eines sicheren Systems mit Hinblick auf die unterschiedlichen Benutzer eines Fahrzeugs (Verkauf, Vermietung, Werkstatt, Einparkservice etc.)

3.4 *Verfahrensprotokoll zum Anlernen eines Schlüssels S2 an das Fahrzeug F1*

P1. Erfolgreiche gegenseitige Authentisierung zwischen einem Besitzerschlüssel BS1* und dem Fahrzeug F1. (Schaffen einer quasi-gesicherten Umgebung für das Anlernen.)

P2. Fahrzeug F1 wird in den Anlernmodus versetzt (z.B. durch eine Abfolge bestimmter Aktionen wie „Blinken – Kuppeln – Blinken").

P3. Schlüssel S2 wird von Fahrzeug F1 ebenfalls in den Anlernmodus versetzt. (I.A. wird dies durch das Senden eines speziellen Kommandos geschehen.)

P4. Schlüssel S2 sendet seinen Bezeichner Id(S2) zum Fahrzeug F1.

P5. Fahrzeug F1 sendet eine Zufallszahl als Startwert für den Pseudo-Zufallszahlengenerator an den Schlüssel S2. Beide Seiten berechnen intern dieselbe Pseudo-Zufallszahl.

P6. Fahrzeug F1 sendet den mittels Pseudo-Zufallszahl verschleierten geheimen Schlüssel an den Schlüssel S2. Der Schlüssel S2 erhält aus der Kenntnis der benutzten Pseudo-Zufallszahl den unverschleierten geheimen Schlüssel K1 und speichert diesen.

P7. Fahrzeug F1 führt eine gegenseitige Authentisierung mit dem Schlüssel S2 durch. Schlägt diese fehl, kann das Verfahren n mal ab Punkt 5 wiederholt werden oder aber sofort abbrechen. Gelingt die anschließende Authentisierung, speichert Fahrzeug F1 den Bezeichner Id(S2).

Bei gelungener Übertragung aller Parameter kann sich fortan auch der Schlüssel S2 erfolgreich bei Fahrzeug F1 authentisieren, d.h. der Besitzer von Schlüssel S2 kann das Fahrzeug F1 nun benutzen wie der Besitzer von S1 auch.

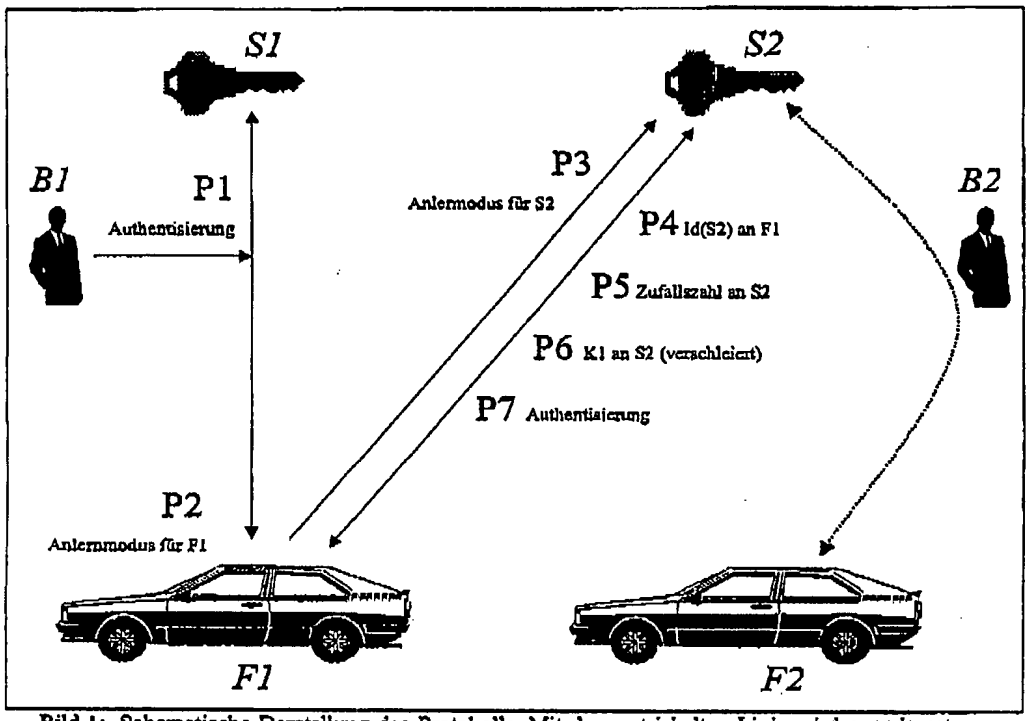

Bild 1: Schematische Darstellung des Protokolls. Mit der gestrichelten Linie wird angedeutet, daß Besitzer B2 nach Durchführung der Prozedur nun zu beiden Fahrzeugen Zugang hat. Falls B1 und B2 identisch sind, benötigt B1 nur noch einen Schlüssel (S2) um beide Fahrzeuge zu bedienen.

3.5 Einschränkungen

Folgende Einschränkungen sind notwendig um die Sicherheit des Verfahrens gewährleisten zu können:

E1. Der an Fahrzeug F1 angelernte Schlüssel S2 ist selbst nicht in der Lage weitere Schlüssel Sx an das Fahrzeug F1 anzulernen, selbst wenn dieser für Fahrzeug F2 ein Besitzer-Schlüssel ist. D.h. der Schlüssel S2 zählt für Fahrzeug F1 nicht als Besitzer-Schlüssel.

E2. Bereits im Fahrzeug F1 gespeicherte Bezeichner Id(Sx) können mit Hilfe eines Besitzer-Schlüssels BS1* gelöscht werden. Damit sind vormals angelernte Schlüssel Sx nicht mehr in der Lage sich beim Fahrzeug F1 zu authentisieren, obwohl diese immer noch den geheimen Schlüssel K1 von Fahrzeug F1 gespeichert haben.

Die Notwendigkeit der beschriebenen Einschränkungen ergibt sich aus folgenden Angriffs-Szenarios gegen die Sicherheit des Systems:

3.6 Angriffs-Szenarios

A1. *Diebstahl des Fahrzeugs F1:* Dies setzt ebenfalls voraus, daß ein gültiger Schlüssel S1* im Besitz des Diebes ist, da er sonst das Fahrzeug nicht benutzen kann. Falls dies sogar ein Besitzer-Schlüssel ist, kann der Dieb andere Schlüssel Sx an das Fahrzeug F1 anlernen (siehe E1). Dies ist nur dann relevant, falls der rechtmäßige Besitzer das Fahrzeug F1 inklusive aller gestohlenen Schlüssel S1* zurückerhält. Die potentielle Gefahr eines erneuten Diebstahls wird durch das Löschen der Bezeichner der angelernten Schlüssel Id(Sx) vermieden (siehe E2).

A2. *Nachschlüssel 1:* Falls eine Werkstatt oder eine andere autorisierte Stelle, welche vorübergehend (rechtmäßig) im Besitz des Fahrzeugs F1 ist, einen Schlüssel Sx an das Fahrzeug F1 anlernen will, wird dies dadurch verhindert, daß der betreffenden Stelle kein Besitzer-Schlüssel überlassen wird (siehe V7). Falls diese Voraussetzung nicht erfüllt sein sollte, kann entweder ein ebenfalls nur an das Fahrzeug F1 angelernter Schlüssel Sx bei der betreffenden Stelle abgegeben werden (siehe E1) oder aber bei Zurücknahme des Fahrzeugs die Bezeichner der unrechtmäßig angelernten Schlüssel Sx im Fahrzeug F1 gelöscht werden.

A3. *Nachschlüssel 2:* Falls der Mieter eines Fahrzeugs F1 sich unberechtigt einen Nachschlüssel anfertigen möchte, kann er dies nur falls er einen Besitzer-Schlüssel S1* mit zum Fahrzeug F1 vom Vermieter erhalten hat (siehe V7). In diesem Fall kann der Vermieter nach Rückgabe des Fahrzeugs mit dem Löschen der Bezeichner eventuell angelernter Schlüssel Sx ein Entwenden des Fahrzeugs F1 durch den ehemaligen Mieter verhindern.

A4. *Verkauf:* Beim Verkauf des Fahrzeugs F1 müssen alle in den Fahrzeugunterlagen vermerkten Schlüssel S1* dem Käufer mit übergeben werden. Der Käufer hat nach dem Kauf die Möglichkeit eventuell noch gespeicherte Bezeichner anderer Schlüssel Id(Sx) zu löschen.

A5. *Nachbestellung von Schlüsseln:* In diesem Fall muß wiederum zwischen Besitzer-Schlüsseln und allen anderen Schlüsseln unterschieden werden: Wird ein Besitzer-Schlüssel nachbestellt, so muß der Bezeichner des als verlorengegangen gemeldete Schlüssel aus dem Fahrzeug gelöscht werden. Ist dies systembedingt nicht möglich, so wird ein kompletter Austausch des Schließsystems durch eine autorisierte Stelle notwendig. Dieser Fall ist auch im „nicht-lernfähigen" System vertreten und die Option des Anlernens wie oben beschrieben trägt nicht zu einer Verringerung der Sicherheit des Systems bei.

Die in den Angriffs-Szenarien für die Automobilbranche typischen Personen lassen sich auch auf Wohnungszugangssysteme übertragen: Hausmeister, Untermieter, Bedienstete etc.

3.7 Bemerkungen

B1. Es ist zweckmäßig, den geheimen Schlüssel K1 von Fahrzeug F1 im angelernten Schlüssel S2 zu speichern. Der Fall, daß im Fahrzeug F1 der geheime Schlüssel K2 von Schlüssel S2 gespeichert wird, widerspricht der Intention, dem Besitzer von Schlüssel S2 Zugang zum Fahrzeug F1 zu gewähren. Die Sicherheit des geheimen Schlüssels K1 ist dabei dadurch gewährleistet, daß

- die Übertragung von K1 an S2 in einer quasi-gesicherten Umgebung abläuft (Authentisierung mittels Besitzer-Schlüssels notwendig),
- der geheime Schlüssel K1 zusätzlich noch verschleiert gesendet wird und
- der Schlüssel S2 niemals dazu veranlaßt werden kann, irgendeinen der gespeicherten geheimen Schlüssel zu übertragen (weder verschlüsselt noch verschleiert oder gar im Klartext).

Außerdem läßt sich mittels eines Besitzer-Schlüssels BS1* der Bezeichner des an das Fahrzeug F1 angelernte Schlüssel S2 wieder löschen und ohne erneute Durchführung obiges Verfahrens nicht wieder speichern.

B2. Die Restriktion E1 legt schon fest, daß Fahrzeuge zwischen Besitzer-Schlüsseln und „Nichtbesitzer"-Schlüsseln unterscheiden können müssen. Damit kann die Zusatzbedingung als sehr wahrscheinlich für ein reales System angenommen werden.

B3. Ein Ansatz über einen Generalschlüssel hätte zur Folge, daß in alle Fahrzeugen Fx und Schlüsseln Sx ein gemeinsamer geheimer Schlüssel GK gespeichert wäre. Damit wäre im kryptographischen Sinne eine Verschlüsselung des zu übertragenen geheimen Schlüssel möglich. Die Sicherheit des Verfahrens beruht dann allein auf der Geheimhaltung des Generalschlüssels. Ein Bekanntwerden dieses Generalschlüssels hätte somit verheerende Folgen für die Sicherheit des gesamten Systems.

4. Vorteile der Erfindung

Die vorgeschlagene Erfindung hat folgende Vorteile:

- Der rechtmäßige Benutzer des Schließsystems erhält die Möglichkeit, flexibel anderen Personen Zugang zu gewähren oder auch wieder zu entziehen.
- Eine Person kann sich für mehrere Schlösser authentisieren lassen, somit wird für Zweitwagen, Zweitwohnungen etc. kein weiterer Schlüssel erforderlich.
- Der Aufwand und damit die Kasten für ein sicheres Schlüsselmanagement sind gering.
- Das vorgeschlagenen Verfahren trägt den besonderen Sicherheitsanforderungen bei Verkauf, Vermietung etc. in einfacher Weise Rechnung.

PATENTANSPRÜCHE

1. Zugangssystem mit originären, autorisierten Zugangsschlüsseln, wobei in dem Zugangssystem und den originären Zugangsschlüsseln jeweils ein identischer, geheimer kryptographischer Schlüssel, jeweils ein identischer kryptographischer Algorithmus und identische Pseudo-Zufallszahlen-Generatoren vorgesehen sind, welche in einem Challenge-Response-Verfahren zur gegenseitigen Authentisierung einsetzbar sind,
dadurch gekennzeichnet,
daß ein oder mehrere zusätzliche, nicht originäre Zugangsschlüssel, die einen Pseudo-Zufallszahlen-Generator gleicher Bauart wie das Zugangssystem aufweisen, in einem Anlermodus in dem Zugangssystem angelernt werden können indem
- mit einem originärem Zugangsschlüssel eine gegenseitige Authentisierung vorgenommen und so eine quasi-gesicherte Umgebung geschaffen wird,
- das Zugangssystem in einen Anlernmodus versetzt wird und dann seinerseits einen anzulernenden, zusätzlichen Schlüssel in einen Anlernmodus versetzt,
- der anzulernende Zugangsschlüssel seinen individuellen Bezeichner, der den Zugangsschlüssel identifiziert, an das Zugangssystem sendet,
- das Zugangssystem den mittels seines Pseudo-Zufalls-Generators verschleierten geheimen kryprographischen Algorithmus an den anzulernenden Zugangsschlüssel sendet, der mittels des in ihm vorgesehenen Zufalls-Generators diesen entschleiert und abspeichert,
- und indem das Zugangssystem eine gegenseitige Authentisierung mit dem angelernten Zugangsschlüssel durchführt, der nachfolgend als Zugangsschlüssel einsetzbar ist.